Shades of Gray: The Evolution of Data Privacy Standards in Higher Education

By Merritt Neale and Matthew Tryniecki

In today's highly connected higher education institutions, there is increasing emphasis placed on information security and data privacy. While the two are inherently linked, they aren't one and the same.

Information security focuses on the prevention and recovery of data breaches; privacy deals more with the applications of personal information, and laws or institutional ethical standards that govern how it is used. To date, a fair amount of focus and investment has been made to better understand the intricacies of information security, but despite this, the privacy landscape in higher education is still relatively unexplored.

In a 2019 EDUCAUSE study, higher education leaders identified privacy as the third most critical IT issue facing the industry, with related concerns around information security and student success coming in at numbers one and two, respectively. Over the last decade, the trend toward technology-enabled "smart" campuses brought with it heightened scrutiny around the ethics and strategy of using student data appropriately. To create formal guidelines for educational institutions, the federal government passed the Family Educational Rights and Privacy Act (FERPA) in 1974, but in today's climate, most experts agree it is outdated and must be revamped to keep pace with a constantly evolving industry.

Since 2013, 41 states have enacted more than 120 supplemental laws. But even these legislative advancements struggle to keep pace with the current rate of technological innovation, driven by rising adoption rates of artificial intelligence and data analytics tools, which often render potentially successful strategies null and void before they can ever be executed.

Data is the lifeblood of any higher education institution's strategic planning activities, providing both evidence of success and justification for new initiatives. And colleges and universities are leveraging this information to make improvements in nearly every area of the institution, including classroom and online learning, recruitment, retention, donor engagement, physical building controls and much more. But this wealth of data is a double-edged sword: on one side, the virtuous applications of data that improve the student experience; on the other, the potential for unethical, ill-advised or unlawful use of personally identifiable information (PII).

Privacy: Safeguarding institutional constituents' privacy rights and maintaining accountability for protecting all types of restricted data

— EDUCAUSE, 2019 IT Issues

Ed Tech and Big Tech

Higher education's increasingly common partnerships with third-party vendors and big technology (e.g., Amazon, Facebook, Google, etc.) further complicate the matter. The involvement of these companies exposes institutions to public scrutiny, fueled by several recent, high-profile violations, as well as ambiguity in terms of who is responsible for what happens to harvested data.

Shadow IT, smart campuses, the internet of things and further proliferation of third-party systems pose a new set of questions at the intersection of privacy and civil liberties, ethics, ownership and autonomy.

Take, for example, the public outcry over the Facebook data sold to Cambridge Analytica, a political consulting firm that allegedly used the information to target American voters in the 2016 presidential election. The blowback from this scandal has caused leaders in nearly every industry to pause and consider the ethical implications of data collection and its potential uses. Some states are even getting in on the action, with Vermont and others approving legislation that governs the sale of citizens' personal data.

Higher education leaders should be mindful of how these types of third-party platforms are used and take initiative to proactively educate students, faculty and staff on what is being collected and how it may be leveraged.

There's No Black and White in Gray Data

Although there is an abundance of ethically neutral or potentially positive uses of students' personal information, there are at least as many gray areas not covered by current legislation, where leaders are being forced to make difficult decisions.

In an article in the Berkeley Technology Law Journal, Christine L. Borgman described gray data as the data that universities collect about members of their community as part of their daily operations that fall outside of the research realm. Some data may still be formally regulated or governed, but the challenge is that often it is not.

For instance, consider the myriad data collection points encountered by college or university students on an average day. Getting home late from a night out, a student may use a campus ID card to enter her dorm. The next morning, feeling pangs of hunger, she uses her dining plan card to pay for breakfast at the cafeteria. Later, she reserves a conference room for that afternoon's organic chemistry study group session. After classes are over, she heads to the soccer field where her performance is tracked by an athlete data management system. And at each stop throughout the day, automated license plate reader (APLR) technology tracks where her vehicle is parked. Multiply these interactions by thousands of students, and one gets a clearer picture of the sheer amount of daily data being collected by these institutions.

Data Collected on the Average Student on a Typical Day

Automated License Plate Technology Tracks Location of Student's Vehicle

Campus ID Card Used to Enter Dorm

Dining Plan Card Used to Pay for Breakfast

System Used to Reserve Conference Room

Performance Tracked by Athlete Data Management System

While the data collected can be helpful when developing a student success strategy, it can also be potentially problematic given the implications of tracking individual students wherever they go on campus.

Gray data challenges can even impact students' post-graduation prospects. Consider the difficult position of athletic administrators determining whether to share a promising student athlete's history of serious head injuries with professional league recruiters.

The use of gray data may conflict with campus privacy standards and notions of academic freedom. But with little to no formal guidance on these types of scenarios, institutions are often left to determine the ethical path forward on their own.

Building the Infrastructure for Data Governance

To meet this challenge head on, institutional standards, policies and guidelines should be collaboratively developed by a diverse and representative group of stakeholders with broad expertise in student privacy and data protection. This collaboration occurs within a well-defined governance structure, with clear roles and responsibilities, and defined outcomes.

To that end, over the last few years, there has been a marked increase in colleges and universities recruiting for chief privacy officers (CPOs) and instating campuswide privacy governance boards.

Chief Privacy Officers

Often relegated to a back-office role on the information security team, effective CPOs transcend this classification by becoming a visible campus ambassador, able to build positive working relationships with diverse stakeholders across all areas of the institution. When a CPO is allowed to be forward-facing, engaging the campus community and the public at large in a dynamic conversation about privacy, real progress can take place.

To be truly successful, these administrators need the tools and sponsorship to create practical guidelines and policies that can translate into daily practices and procedures.

But CPOs should not be the sole arbiters of an institution's privacy policy. They must be willing and able to bring in other internal and external experts to help them make informed and educated decisions. At the same time, they must also be viewed as a valuable, accessible resource for stakeholders across the institution.

Privacy Governance Boards

With the goal of promoting a balance of perspectives from across the institution, formal privacy governance boards are essential to the ethical review and adjudication of complex information and data management matters. These committees are typically composed of a mix of knowledgeable faculty and administrators, while some integrate students as well.

The University of California Los Angeles (UCLA) has its Board on Privacy And Data Protection, while the University of Chicago looks to its Data Stewardship Council for guidance.

In combination with an institution's privacy office, these boards can help demystify the niche student privacy and data protection concerns inherent in the daily operations of colleges and universities.

The Future of Privacy in Higher Education

In the future, higher education leaders will continue to grapple with new challenges and gray areas regarding student privacy. In addition, there will likely be an upsurge in state legislation — with California's Consumer Privacy Act leading the way (set to take effect January 1, 2020) — as well as increased rigor around enforcing existing federal laws like FERPA, the Health Insurance Portability and Accountability Act (HIPAA) and Europe's General Data Protection Regulation (GDPR).

With an uptick in these formal regulations will come additional ambiguity as prevailing laws already contradict each other in some cases; some require the long-term storage of data while others mandate concepts like the GDPR's "right to be forgotten," wherein consumer information must be erased if requested.

Today, most institutions are just beginning to invest in the resources required to respond effectively to these developments. Privacy offices, while increasingly common in higher education, are still relatively rare. And those that are in place are often understaffed and mired in everyday activities, including breach response, contract reviews and compliance activities.

Likewise, data governance boards are increasing in number, yet many still struggle to make a significant impact on institutional policies. Driving consensus across a wide range of stakeholder groups is a difficult task, often pitting faculty against administration, but leaders have a moral, ethical and professional responsibility to find common ground for the greater good of the institution.

Forward-thinking institutions will embrace this new frontier in higher education by building a robust infrastructure to support ethical data usage, privacy education and innovation.

Steps for Improving Your Institution's Management of Data Privacy

Consider the following steps to get started on improving your data governance:

- Get familiar with existing laws (e.g., HIPAA, GDPR and the California Consumer Privacy Act, to name a few).
- Conduct an asset inventory to identify where the institution is storing personal information as part of its operations.
- Assess the institution's potential risks related to data privacy to help prioritize opportunities for improvement.
- Clearly define ownership for key privacy areas to ensure role clarity and effective execution.

Key Takeaways

Think differently.

In light of the many gray areas related to student privacy, consider whether the establishment of a privacy office and other governance constructs would help your institution navigate this ambiguity more effectively.

Plan differently.

Ensure your governance structure supports diverse stakeholder participation in the review and adjudication of complex privacy matters.

Act differently.

Empower your privacy office and/or data governance board to create supplemental guidance and policies to cover gray data concerns.

huronconsultinggroup.com